I claim:

1. A method of bypassing a programmable processing element, the method comprising:

examining data, the data including at least a header;

removing the header from the data;

encrypting the data through a cryptographic component;

rejoining the removed header and the encrypted data; and

outputting the rejoined header and encrypted data.

2. The method of bypassing a programmable processing element of claim 1, wherein the programmable processing element is at least one FPGA.

3. The method of bypassing a programmable processing element of claim 1, wherein the data further includes an Internet protocol header.

4. The method of bypassing a programmable processing element of claim 1, wherein the data further includes an internal Internet protocol header.

5. The method of bypassing a programmable processing element of claim 1, wherein the data is at least one of speech data, Ethernet data, or IC5232 data.

6. The method of bypassing a programmable processing element of claim 1, wherein the header is transferred around the cryptographic component.

7. The method of bypassing a programmable processing element of claim 6, wherein the cryptographic component is an encrypting algorithm.

8. The method of bypassing a programmable processing element of claim 1, wherein the examining data occurs at traffic rates.

9. The method of bypassing a programmable processing element of claim 1, wherein the removing the header occurs at traffic rates.

10. The method of bypassing a programmable processing element of claim 1, wherein the encrypting the data occurs at traffic rates.

11. The method of bypassing a programmable processing element of claim 1, wherein the rejoining the removed header and the encrypted data occurs at traffic rates.

12. The method of bypassing a programmable processing element of claim 1, further comprising validating the data.

13. The method of bypassing a programmable processing element of claim 1, wherein the validating the data includes checking at least one of the header format, number of bits, contents, and details.

14. A programmable processing element, the element comprising:

examination logic, the examination logic examining the input data, the input data including at least a header;

separation logic, the separation logic removing the header from the examined data, the header being transferred outside an encryption component;

the encryption component, wherein the encryption component includes a cryptographic element such that the data can be encrypted; and

merge logic, the merge logic rejoining the removed header and the encrypted data to be output.

15. The programmable processing element of claim 14, wherein the programmable processing element is at least one FPGA.

16. The programmable processing element of claim 14, further comprising:

validation logic, the validation logic determining whether to encrypt the data.

17. The programmable processing element of claim 16, wherein the validation logic checks at least one of the header format, number of bits, contents, and details.

18. The programmable processing element of claim 14, wherein the data further includes an Internet protocol header.

19. The programmable processing element of claim 14, wherein the data further includes an internal Internet protocol header.

20. The programmable processing element of claim 14, wherein the examination logic operates at traffic rates.

21. The programmable processing element of claim 14, wherein the separation logic operates at traffic rates.

22. The programmable processing element of claim 14, wherein the merge logic operates at traffic rates.

23. The programmable processing element of claim 14, wherein the data is at least one of speech data, Ethernet data, or IC5232 data.